UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/743,119	12/22/2003	W. Carey Bunn	END920030045US1	7503

26502 7590 09/09/2010

IBM CORPORATION
IPLAW SHCB/40-3
1701 NORTH STREET
ENDICOTT, NY 13760

EXAMINER	
SCHMIDT, KARI L	
ART UNIT	**PAPER NUMBER**
2439	
NOTIFICATION DATE	**DELIVERY MODE**
09/09/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

endiplaw@us.ibm.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte W. CAREY BUNN, LETITIA K. CALVERT, and
MARY E. KARNES

Appeal 2009-004174
Application 10/743,119[1]
Technology Center 2400

Before JOSEPH F. RUGGIERO, MARC S. HOFF,
and THOMAS S. HAHN, *Administrative Patent Judges*.

HOFF, *Administrative Patent Judge*.

DECISION ON APPEAL[2]

[1] The real party in interest is International Business Machines Corporation.

[2] The two-month time period for filing an appeal or commencing a civil action, as recited in 37 C.F.R. § 1.304, or filing a request for rehearing, as recited in 37 C.F.R. § 41.52, begins to run from the "MAIL DATE" (paper delivery mode) or the "NOTIFICATION DATE" (electronic delivery mode) shown on the PTOL-90A cover letter attached to this decision.

STATEMENT OF THE CASE

Appellants appeal under 35 U.S.C. § 134(a) from a Final Rejection of claims 1-20. We have jurisdiction under 35 U.S.C. § 6(b).

We reverse.

Appellants' invention relates to a method for providing network perimeter security assessment that involves a combination of perimeter security assessment disciplines. Specifically, a security review of a network perimeter architecture is performed along with a review of (1) the security of data processing devices that transfer data across the perimeter of the network, (2) the security of applications that transfer data across the perimeter and (3) the vulnerability of applications or data processing devices within the perimeter from computers or users outside of the perimeter. Each of the reviews may be performed by comparison to a security policy of an enterprise that owns or controls the network and a report may be generated based upon all the reviews (Abstract).

Claim 1 is exemplary:

1. A method for checking network perimeter security, said method comprising the steps of:

reviewing security of a network perimeter architecture;

reviewing security of data processing devices that transfer data across the perimeter of the network;

reviewing security of applications that transfer data across said perimeter;

reviewing vulnerability of applications or data processing devices within said perimeter from computers or users outside of said perimeter; and

generating a report concerning security of said perimeter based upon all of the reviewing steps.

The prior art relied upon by the Examiner in rejecting the claims on appeal is:

Bunker	US 2003/0028803 A1	Feb. 6, 2003

Claims 1-20 stand rejected under 35 U.S.C. § 102(b) as being anticipated by Bunker.

Rather than repeat the arguments of Appellants or the Examiner, we make reference to the Appeal Brief (filed Feb. 19, 2008) and the Examiner's Answer (mailed April 28, 2008) for their respective details.

ISSUE

Appellants contend that Bunker merely discloses a methodology for determining the vulnerability of a customer system by launching numerous basic tests that simulate hackers attempting to harm the customer system (App. Br. 7). Appellants contend that Bunker only discloses vulnerability testing, rather than reviewing security of network perimeter architecture, data processing devices, or applications as the claims require (App. Br. 8-9).

Appellants' contentions present us with the following dispositive issue: Does Bunker disclose reviewing security of the network perimeter architecture?

FINDINGS OF FACT

The following Findings of Fact (FF) are shown by a preponderance of the evidence.

The Invention

1. The first step in the network architecture review is to perform a design review against the environment to understand how network connections are created. Specifically, architecture diagrams are obtained and different elements, such as data flow, OSI layer separation, identity control methods, including authorization and entitlement, auditing and authentication of the architecture are reviewed. The network architecture and design are then compared against corporate standards and industry best practice benchmarks. Finally, a review of the tools and techniques used to authorize and control access to the environment is conducted. Specific tests are identified which are used to attempt to circumvent the security controls of the environment. In addition, the network gateway design is tested to verify whether it can restrict access to the specifically authorized IT resource(s) (Figs. 1, 4, and 6; Spec. 12:11-20 and 15:10-14).

Bunker

2. Bunker discloses a network vulnerability assessment system and method wherein real-time network security vulnerability assessment tests, possibly complete with recommended security solutions are conducted. External vulnerability assessment tests may emulate hacker methodology in a safe way and enable study of a network for security openings, thereby gaining a true view of risk levels without affecting customer operations (Abstract).

3. Bunker discloses a sample of the attack logic used by the preferred embodiment that includes a first "wave" 1410 of basic tests 516, and an initial mapping 1402 that records a complete inventory of services running on the target network 1002. The initial mapping 1402 discloses what systems 1102 are present, what ports are open (1404, 1406, and 1408), what services each system is running, general networking problems, web or e-mail servers, and whether the system's IP address is a phone number. Basic network diagnostics that are run might include but are not limited to whether a system can be pinged, whether a network connection fault exists, and whether rerouting is successful (Fig. 14; [0181]).

PRINCIPLES OF LAW

Anticipation pursuant to 35 U.S.C § 102 is established when a single prior art reference discloses expressly or under the principles of inherency each and every limitation of the claimed invention. *Atlas Powder Co. v. IRECO Inc.*, 190 F.3d 1342, 1347 (Fed. Cir. 1999); *In re Paulsen*, 30 F.3d 1475, 1478-79 (Fed. Cir. 1994).

ANALYSIS

Claim 1-20

Independent claim 1 recites “reviewing security of a network perimeter architecture.” Independent claims 16 and 18 recite a similar claim limitation.

We consider Appellants’ arguments to be persuasive to show Examiner error. Specifically, we do not agree with the Examiner’s finding that Bunker discloses “reviewing security of a network perimeter architecture" (Ans. 22). Bunker discloses a multiple wave vulnerability testing assessment system and method that includes an initial mapping which records a complete inventory of services running on a target network including what ports are open (FF 2 and 3). Bunker does not disclose that a security assessment is performed for all nodes within the network architecture, including servers, clients, peripheral devices, and entries and exits from the network (see FF 3). Bunker discloses that the system only maps the services and open ports, but does not define all the nodes in the architecture (FF 3). As shown in Figure 1 of the Specification, a network architecture includes more than just server machines that make their services available using ports (FF 1). More particularly, that architectural review process as disclosed in the Specification includes first obtaining an architecture diagram 610 (FF 1). Next, within the process of reviewing the architecture, review of the data flow and OSI layers 2-7 occurs, along with identifying control methods: such as authorization, entitlement, auditing, and authentication in step 620 (FF 1).

Therefore, we find that Bunker does not disclose "reviewing security of a network perimeter architecture." As a result, we will not sustain the Examiner's rejection of independent claims 1, 16, and 18 and that of dependent claims 2-15, 17, and 19-20 under 35 U.S.C. § 102(b), we reverse the Examiner's rejection.

CONCLUSION

The reference does not disclose reviewing security of the network perimeter architecture.

ORDER

The Examiner's rejection of claims 1-20 is reversed.

REVERSED

ELD

IBM CORPORATION
IPLAW SHCB/40-3
1701 NORTH STREET
ENDICOTT, NY 13760